UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/787,065	07/26/2001	Florian Oelmaier	3118	6076

22862 7590 01/24/2008
GLENN PATENT GROUP
3475 EDISON WAY, SUITE L
MENLO PARK, CA 94025

EXAMINER	
PICH, PONNOREAY	
ART UNIT	PAPER NUMBER
2135	
MAIL DATE	DELIVERY MODE
01/24/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 09/787,065	**Applicant(s)** OELMAIER ET AL.
	Examiner Ponnoreay Pich	**Art Unit** 2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 November 2007*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) *17 and 18* is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

This application contains claims 17-18 drawn to an invention nonelected without traverse in the reply filed on 5/24/07. A complete reply to the final rejection must include cancellation of nonelected claims (37 CFR 1.144) See MPEP § 821.01.

Claims 1-16 submitted on 11/7/07 were examined.

Response to Arguments

Applicant's arguments submitted on 11/7/07 were fully considered, but were not persuasive.

The Applicant argues that Effing does not disclose a device for determining the operational data of the electronic circuit, said data being influenced by an operation of the electronic circuit when the circuit executes the algorithm. The examiner respectfully disagrees.

The examiner submits that measuring circuit 54 of the identity card seen in Figures 10 and 11 meet this limitation since it measures/determines the programming time/individual characteristics of a memory (col 11, lines 54-58). The individual characteristic can be considered operational data and is obtained by executing an algorithm which programs the card's memory cells, measures the programming time for individual memory cells, and encrypts it to determine if an identity card is authentic or not (col 2, lines 1-45 and col 12, lines 5-35). As such, the operational data M is influenced by an operation of the card/electronic circuit when the card executes the aforementioned algorithm and the operational data is used to create the output, i.e. encrypted M (col 12, lines 5-20).

Applicant argues that Effing's teachings differ from the claimed present invention because the individual characterizing data in memory is always the same and can therefore be stored at the beginning, whereas according to the present claimed present invention, the operational data depends on the input data and therefore a single storage of the operational data would not make sense.

The examiner respectfully submits that there is nothing recited in claim 1 which prohibits the input data from always being the same values. Assuming the same input values are always used and the same algorithm is always used, one would always get the same operational data and the same output. There is also nothing recited in the claim which prohibits the operational data from being stored in the device after a first execution of the algorithm. As such, claim 1 as currently recited is broad enough to be anticipated by Effing.

Applicant argues that it is not correct to say that Effing's programming time is an operational data of the electronic circuit which is influenced by an operation of the electronic circuit when the electronic circuit executes the algorithm. Applicant argues that the programming time of an EEPROM does not depend on the input data. The examiner respectfully disagrees with both these arguments.

First it is noted that with respect to the recited algorithm, claim 1 only requires that the algorithm generates an output data on the basis of input data and that it uses the operational data in generating the output data. As such, one can interpret Effing's teachings of programming the memory, measuring the programming time, and encrypting the programming time as equivalent to the claimed algorithm. Further, it is noted that Effing's invention relies upon the fact that due to manufacturing differences, it is impossible for two different circuits to have the same programming time. What one should understand though is that in programming the memory to test for its authenticity is that the same input data must be used each time for comparing programming time. If one did not, there is no way to guarantee that the same programming time would be achieved even if it was the same card. Since the programming time is dependent on the input data used to program the memory and on the structure of the memory, the programming time can be considered operational data of the electronic circuit. Since one cannot get the programming time unless the circuit operates to execute the aforementioned algorithm, the programming time/operational data is influenced by an operation of the electronic circuit when the electronic circuit executes the algorithm. As per the argument that the programming time of an EEPROM does not depend on the input data, the examiner respectfully disagrees because it is inherent that any type of memory's programming time is dependent on the data used to program it and on the structure of the memory that the data is programmed onto. A data 1K in size for example is going to take much less time to program into memory than one which is 100MB in size. Further, the structure of cache memory for instance is such that it allows much faster read/write than memory used in hard drives. As such, contrary to applicant's assertions, the examiner's reasoning presented the last office action was correct.

Applicant argues that Effing does not disclose operational data are detected which are influenced by an operation of the electronic circuit when the electronic circuit executes the algorithm, where the operational data depends on the input data. The examiner respectfully disagrees. As discussed above already, the programming time is considered operational data and is detected by measuring circuit 54. If the identity card did not execute the algorithm discussed above, the programming time could not be measured, thus it is influenced by an operation of the electronic circuit when the electronic circuit executes the algorithm, where the operational data/programming time depends on the input data, i.e. the data used to program the memory and the memory's structure.

Applicant's arguments to claims 2, 11-13, and 15 are directed at dependency and are traversed due to the arguments of claim 1 being traversed.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 3-5, 7-10, and 16 are rejected under 35 U.S.C. 102(b/e) as being anticipated by Effing (US 5,818,738).

Note that Effing qualifies as a 102(e) reference and a 102(b) reference because it was first published as document WO 89/04022 on 5/5/1989 and later as document US 5,818,738 on 10/6/1998.

Claim 1:

Effing discloses:

1. An electronic circuit (i.e. identity card as seen in Figure 1 having encryption unit 60 as seen in Figures 10 and 11) for executing an algorithm that generates the output data (i.e. encrypted M or M) on the basis of the input data, i.e. data used to program the card's memory to get M (col 2, lines 37-40; col 4, lines 61-64; col 5, lines 17-38; col 12, lines 5-20; and col 15, lines 59-64). *The card programming its memory, measuring the programming time to get a characteristic M, and encrypting M is considered execution of an algorithm.*
2. A unit (i.e. measuring circuit 54) for detecting operational data (i.e. programming time/individual characteristics M) of the electronic circuit which are influenced by an operation of the electronic circuit (col 8, lines 13-16; col 11, lines 11-34 and 54-58; and col 12, lines 6-10) when said electronic circuit executes the algorithm, the operational data depending on the input data (col 7, lines 1-5). *Programming time of a memory is inherently dependent on the structure of the memory and on the data used to program the memory.*

3. The unit for detecting operational data being coupled to the electronic circuit in such a way that the operational data of the electronic circuit are used by the algorithm, which is executed by said electronic circuit, for generating the output data (col 12, lines 5-20 and Figures 10-11, item 51).

Claim 3:

Effing further discloses wherein the electronic circuit and the unit for detecting operational data are integrated as a unit (Figures 10-11, item 51). The unit for detecting (i.e. measuring circuit 54) is part of the electronic circuit (i.e. card 51), thus the electronic circuit and the unit for detecting are integrated as a unit.

Claim 4:

Effing further discloses wherein the device is contained in a smart card or a PC card (Figures 10-11, item 51).

Claim 5:

Effing further discloses wherein the electronic circuit is arranged so as to execute a cryptoalgorithm (col 12, lines 5-20 and col 14, lines 33-38).

Claim 7:

Effing further discloses wherein the cryptoalgorithm is a multi-step algorithm, the operational data of one algorithm step being used as input data for the subsequent algorithm step (col 5, lines 51-57).

Note that Effing discloses that the cryptoalgorithm used could be DES. DES is a multi-step algorithm in which data from a one step is used as input into the next step.

Claim 8:

Effing further discloses wherein the electronic circuit is arranged so as to stop the operation after a predetermined time during execution of the algorithm (col 2, lines 37-45 and col 2, line 65-col 3, line 3) and wherein the detection unit is arranged so as to feed operational data into the algorithm at said predetermined execution time (col 10, lines 60-65 and col 12, lines 6-20).

Claim 9:

Effing further discloses wherein the algorithm is of such a nature that it will first randomize the input data, whereby the dependence of the operational data on the input data will be pseudo-random (col 5, lines 51-57 and col 12, lines 5-12 and 63-67).

Claim 10:

Effing further discloses wherein the output data generated by the algorithm are the only operational data (col 12, lines 5-20).

Claim 16:

Effing further discloses wherein the operational data detection unit comprises a pattern recognition algorithm so as to produce the operational data from power or time parameters of the electronic circuit (col 2, line 66-col 3, line 20 and col 8, lines 13-16).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2, 11-13, and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Effing (US 5,818,738) in view of Kocher et al (Us 6,298,442).

Claim 2:

Effing further discloses wherein the operational data is selected from the group comprising time data (col 2, lines 37-45; col 11, lines 54-58; and col 12, lines 6-10). Effing does not explicitly disclose power data is part of the group from which operational data is selected.

However, Effing discloses that it has been known for some time to test the authenticity of data storage carriers by measuring characteristics which are unique to the data carrier (col 1, lines 11-15 and col 2, lines 1-11). These unique characteristics come from it being impossible to manufacture data carriers which are exactly identical in physical nature. As a result, of these physical differences, different data carriers may require different amounts of time to carry out the same algorithm, for example (col 2, lines 22-44). Further, Kocher discloses that at the time applicant's invention was made, both time and power monitoring attacks could be used to determine the values of keys stored in a data carrier (col 2, lines 5-24). One skilled should appreciate that power is a measurement of the amount of energy consumed per unit time. Since it is possible according to Effing's teachings to use the measurement of the amount of time to perform a particular algorithm to authenticate a particular data carrier, then it would have been obvious to one of ordinary skill in the art based on the additional teachings of Kocher that one can also authenticate the data carrier by measuring the amount of power consumed by a particular data carrier. If the amount of time it takes to execute a particular algorithm can vary from data carrier to data carrier due to physical differences brought about during manufacture, then the amount of power consumed would also be expected to be different due to the physical differences.

As such, at the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to modify Effing's invention such that power data was also chosen operational data. One skilled would have been motivated to do so because it would have been obvious to one of ordinary skill to try different ways of measuring the physical differences of a data carrier for authentication purposes. One skilled would have known that power is a measure of energy used per unit time and because the physical characteristic differences could cause a difference in the amount of time it takes to execute a particular algorithm, it would be expected to also cause a difference in the amount of power consumed. Based on Kocher's teachings, it was known to use both timing and power monitoring attacks to determine a stored key. Since Effing used time monitoring for authentication, it would have occurred to one skilled in the art to at least try monitoring power for authentication.

Claim 11:

Effing further discloses wherein the electronic circuit comprises two sub-circuits which execute a sub-algorithm, the first sub-algorithm being a test algorithm whose operational data are detected by the detection unit (col 2, lines 37-45 and col 8, lines 13-16), and the second sub-algorithm being a cryptoalgorithm or a checksum algorithm, the operational data of the test algorithm being processed in the cryptoalgorithm (col 12, lines 5-20).

Claim 12:

Effing further discloses wherein the second sub-circuit is arranged so as to execute the DES algorithm which comprises n steps, and wherein the first sub-circuit is arranged as to execute a test algorithm which is also n steps, the input data being adapted to be fed into the first step of the DES algorithm as well as into the first step of the test algorithm, and data which are adapted to be fed into a further step of the DES algorithm being result data of the first step of the DES algorithm and operational data of the first step of the test algorithm, whereas a result of one step of the test algorithm is rejected (col 5, lines 51-57; col 8, line s13-24; and col 12, lines 5-20).

Claim 13:

Effing further discloses wherein the operational data detection unit comprises a time measuring means for measuring the time which the electronic circuit needs for executing a specific task when said specific task is being executed (col 8, lines 13-16 and col 8, lines 50-56).

Effing does not explicitly disclose wherein the operational data detection unit also comprises a power measuring means for measuring the power consumed when said specific task is being executed. However, as discussed in claim 2, it would have been obvious to one of ordinary skill in the art to measure the physical characteristics of the data carrier via time and/or power measurement. As such, it would have been obvious to one of ordinary skill in the art to modify the operational data detection unit of Effing's invention according to the limitations recited in claim 13 by having it also comprise a power measuring means for measuring the power consumed when said specific task is being executed. One of ordinary skill would have been motivated to do so because a power detection means would be required to detect the amount of power consumed to authenticate if the data carrier disclosed by Effing is authentic or not. One of ordinary skill would have been motivated to use power consumption detection to authenticate the data carrier for the reasons discussed in claim 2.

Claim 15:

Effing further discloses wherein the time measuring means comprises an internal clock generator (col 8, lines 13-16).

Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Effing (US 5,818,738) in view of Kocher et al (Us 6,298,442) in further view of Faulkner (US 4,788,494).

Claim 14:

Effing does not explicitly disclose wherein the power measuring means comprises a resistor, a capacitor and an analog-digital converter for measuring power consumed. However, the limitation is disclosed by Faulkner (Fig 2-3; col 4, lines 56-57; and col 6, lines 21-24 and 55-59).

At the time applicant's invention was made, it would have been obvious to one skilled in the art to further modify Effing's invention such that the power measuring means comprises a resistor, a capacitor and an analog-digital converter for measuring power consumed. One skilled would have been motivated to use the type of power measuring means disclosed by Faulkner because it is low cost (col 2, lines 28-32).

Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Effing (US 5,818,738) in view of Angelo (US 5,887,131).

Claim 6:

Effing does not explicitly disclose wherein the electronic circuit is arranged so as to execute a checksum algorithm. However, note that the purpose of Effing's invention is authentication by having a host device (i.e. Fig 11, item 52) validate an encrypted value sent from the IC card to the host device. Angelo discloses use of a checksum algorithm for authentication purposes (abstract).

At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to modify Effing's invention according to the limitations recited in claim 6 by having the electronic circuit execute a checksum algorithm in place of the encryption algorithm. One skilled would have been motivated to do so because use of checksum algorithms in authentication is faster than many other popular encryption algorithms (Angelo: col 7, lines 49-53). Note that use of a checksum algorithm in authentication is also more secure than plain encryption of a value to be compared.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Thurs.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Ponnoreay Pich
Examiner
Art Unit 2135

PP

KIM VU
[illegible] PATENT [illegible]
[illegible]OLOGY CENTER [illegible]